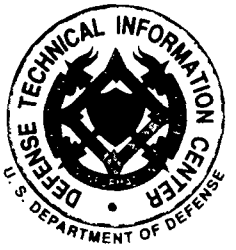

Defense Technical Information Center Compilation Part Notice

This paper is a part of the following report:

- *Title:* Technology Showcase: Integrated Monitoring, Diagnostics and Failure Prevention. Proceedings of a Joint Conference, Mobile, Alabama, April 22-26, 1996.

- *To order the complete compilation report, use:* AD-A325 558

The component part is provided here to allow users access to individually authored sections of proceedings, annals, symposia, etc. However, the component should be considered within the context of the overall compilation report and not as a stand-alone technical report.

A MODEL-BASED FAILURE DETECTION, ISOLATION AND RECOVERY SYSTEM

Amit Misra and Janos Sztipanovits
Department of Electrical and Computer Engineering
Vanderbilt University
Box 1824, Station B
Nashville, TN 37235
email : misra@vuse.vanderbilt.edu

Abstract: The Failure Detection, Isolation and Recovery (FDIR) in the International Space Station Alpha (ISSA) requires timely monitoring and diagnosis of failures so that recovery actions can be employed to safeguard the mission and the life of crew. Using traditional methods for representation of domain knowledge and for diagnosis proves to be ineffectual because of the scale, complexity and dynamics of ISSA. Model-based approach for representing systems and for diagnosis is an attractive and feasible solution. We have developed and field tested a model-based real-time robust monitoring and diagnostic system for ISSA and other aerospace systems. The system is represented using hierarchical and multiple-aspect models, which include representation of functional structure as well as the physical component assemblies. A discretized model of the failures and their effects is represented using timed failure propagation graphs. The monitoring mechanism is modeled by using a discretized sensor space, with mechanisms for sensor validation. The diagnostic reasoning applies structural and temporal constraints for the generation and validation of fault hypotheses using the "predictor-corrector" principle. The diagnosis is generated in real-time amid an evolving alarm scenario, and uses progressive deepening control strategy. The robust diagnostic system has been tested and demonstrated using ISSA models obtained from the Boeing Company.

Key Words: Diagnostics; fault models; hierarchical models; model-based systems; multiple aspects; program synthesis; sensor failure

INTRODUCTION: An increasingly competitive aerospace market requires requires computer integrated Failure Detection, Isolation and Recovery (FDIR) systems to perform complex and sophisticated analyses that are capable of providing real-time embedded vehicle health management. Simultaneously, a general trend in the evolution of complex, large-scale, computer integrated systems is the rapidly increasing use of design-time models in system operation. The goal is to synthesize vehicle health management systems that are formally and automatically derived from the integrated model sets developed during the vehicle design, development, build, test, and verification.

In this paper we describe a model-integrated approach to synthesis of FDIR system for aerospace vehicles. The model-integrated approach is based upon the MultiGraph Architec-

ture (MGA) [15]. The primary specifications for FDIR come from the International Space Station Alpha (ISSA) program requirements, though FDIR tools and formalisms described here could be applied (with appropriate modifications) to task of health management for most large-scale, complex, computer integrated system. The FDIR system consists of modeling formalisms and a health management system, synthesized from the models of the artifact.

FDIR MODELING PARADIGM: It is evident that the practical use of a model-integrated system is limited by the "goodness" of the models themselves, which in turn is influenced by the formalism used for modeling. Thus, one must develop modeling formalisms that capture the essence of the system being modeled *and* the FDIR requirements. One must also recognize the fact that there is a critical need for software technology which makes high-performance computing and communication capabilities accessible for end-users. Systems engineers need domain-specific modeling and analysis environments that support the building and verification of vehicle fault models, provide interfaces to engineering databases and systems engineering tools, and allow the synthesis of FDIR systems that are consistent with the vehicle models. Further, there typically are some mature engineering disciplines underlying the design and systems engineering. Thus, the modeling paradigms are not "negotiable": systems engineers need to be supported by rich, domain specific concepts, relations, and composition principles routinely used in the field.

The main challenges in using a model-based approach for the FDIR in large-scale heterogeneous dynamic systems are the following :

1. The size of the systems in terms of the number of components, the complexity of physical processes and their interactions can be large. In providing models for system-wide diagnosis, *scaleability* of the modeling technique becomes a major issue.

2. Design of such systems involves different engineering disciplines with different focus and tools. In the FDIR modeling four such disciplines are identified – signal, fluid, electrical, mechanical.

3. The source of failures may be outside of the system boundary. Propagating effects of *external disturbances* must be traced.

4. The primary goal of diagnosis in critical systems is the prevention of the occurrence of critical failures. Prediction of the propagation of discrepancies requires not only the spatial but also the *temporal isolation of fault events.* For this purpose, steady-state models are often useless, because processes may only slowly converge to steady-state and because steady-state models do not capture the dynamics of fault propagation.

5. Fault diagnosis is based on the observation of the behavior of the plant during a fault incidence. Consequently, the models to be used in fault diagnosis should capture the dynamic behavior of processes when it is out of the normal operation range. Needless to say, *modeling uncertainties* in these regions are even more significant than in the normal operation range.

6. The FDIR system must be able to reason about *abrupt* faults and input disturbances, which means that assumptions about the system (valid only during normal operation) become invalid and unusable.

7. Faults propagate through the system. That is, the effects of a fault rarely tend to be localized unless specific measures are taken. The goal of FDIR is to contain and rectify the faults locally. Thus the propagating effects of faults must be modeled.

The first two challenges listed above address the issues common to all complex, heterogeneous, large-scale system, more or less independently from the application. In other words, these issues are not specific to FDIR, but arise in control, simulation and many other applications, and relate to the formalisms used for overall organization of *system models*. The rest of the challenges listed above arise out the FDIR task specifically. These issues are addressed in the formalisms used for *fault models*, which are a subset of system models. We will first give an overview of the organization of system models, followed by a description of the fault models.

Hierarchical, Multiple Aspect, Discipline Oriented System Models: Because our goal is to model engineering systems, the modeling technique should utilize the well known engineering techniques to manage complexity.

One of the primary model structuring method is focusing on selected types of interactions; i.e. to model a system from *multiple aspects*. Different modeling aspects use different concepts (e.g. the physical structure is defined in terms of assemblies and sub-assemblies, while the functional structure of a temperature control system is defined in terms of material and energy flows). Each aspect may simultaneously be sub-divided into *views*, that contain discipline oriented information. The models are typically organized into *decomposition hierarchies* controlling the level of details shown. On each level, the system is modeled as an aggregate of connected sub-systems. The type of the connections are determined by the modeling aspect and view. The subsystems are connected through an *interface*, which defines their boundaries and separates the internal and external environments. The decomposition hierarchies and the connected set of subsystems on each level constitute the *structural model* of the system. Each subsystem can also be characterized in terms of the relationships among its input/output quantities. These models are called *behavioral models*.

For purposes of FDIR, the system models are broken down into two primary hierarchies – the physical assembly, which models the components in the system, and the functional decomposition. The physical models and the functional models are both described in terms of their structure and behavior. Separation of the functional and physical structure is an essential difference from the primarily component-oriented modeling in model-based diagnostic systems (e.g. [1, 2, 3]). Our rationale for this separation is the following :

1. There are many examples for multi-function components that are involved in the implementation of several functionalities in the same time. Well known examples are computers and energy distribution systems.

Table 1: Physical Model Aspects

Aspect	Concept(s) Modeled	Model Elements
Assembly Aspect	Component assemblies and energy and material flows.	Sub-component and input and output flows.
State Transitions Aspect	Operation states and State Transition Machine	Component states, sub-states, state transitions, local, input and output events.
Alarm Generation Aspect	Sensors	Alarms that the sensor generates, and sensor attributes like cost and time to use, probability of false alarm, etc.
Component Faults Aspect	Faulty behavior	Failure modes and failure rates of components.

2. Assignments among physical components and functionalities are not always static. Physical redundancy and the use of multiple-function components are frequently used to achieve fault tolerance in critical systems.

Both the physical and functional models have many different aspects. In this paper we present only a very brief description of the different modeling aspects of physical and functional models, given in Table 1 and Table 2. For a more detailed description, the reader is referred to [14].

Fault Modeling: Model-based diagnostic systems work with a model (a suitable representation) of the system. The level of detail in the models can be kept at the level required by the FDIR requirements. These diagnostic systems interpret the observed discrepancies in the context of the system model. There are primarily two kinds of models that have traditionally been used for diagnosis – *functional models* and *fault models.*

Functional models (also called behavioral models) describe the "correct" behavior of the system, i.e., how the system is supposed to behave when no faults are present. The level of abstraction in the functional models can vary from system to system, depending on the application – from quantitative models (also called *analytical* models) using state-space representation to qualitative models.

Quantitative functional models (analytical models) use Ordinary Differential Equations (ODE), state-space or similar representations (examples of such systems can be found in [11, 12, 13], among others), to diagnose anomalies. However, the usefulness of analytical models is limited to small, stable sub-systems only, which have a well defined and simple domain theory, as opposed to the large-scale, complex systems addressed in this paper.

Table 2: Functional Model Aspects

Aspect	Concept(s) Modeled	Model Elements
Structure Aspect	Functional structure and energy and material flows	Sub-functionalities and input and output in the four disciplines (signal, fluid, electrical and mechanical).
State Transitions Aspect	Operation states and State Transition Machine	Functionality states, substates, state transitions, local, input and output events.
Failure Propagations Aspects	Failure interactions	Component failure modes, functional discrepancies and timed failure propagations.
Failure Observation Aspect	Fault monitoring	Alarms and sensor states.
Implementation Aspect	Relationship between functionalities and components in the system	The physical components that fulfill the functionality and the redundancy between the components.

To address the complexity in most engineering systems, some researchers have used *qualitative* functional models. Qualitative functional models divide the process variable space into "ranges of interest" and use qualitative physics to generate the behavior of a system. They have met with varying degrees of success in analyzing and predicting the complete and correct behavior. The functionality can be described using just input/output relationships as in [4], using a mathematical description, or using a set of connected components and causal sequences which give a description of how the system behaves [1, 2, 3].

Using functional models to diagnose faults has its own problems, the foremost being the accuracy and validity of models, particularly if faults are present. Further, while the models might be good for identifying the presence of a malfunction (using simulation or analytical methods), they are not necessarily helpful in diagnosing, i.e., locating the faulty component. This is because using functional models can lead to an explosion in the size of the diagnostic search space and hence the number of possible hypotheses, thereby rendering diagnosis intractable. The large diagnostic search spaces arise out of the attempt to reason about *abnormal* behavior of a system using models that describe the behavior under *normal* conditions. Except in limited cases, such attempts have not been successful.

Fault models (fault trees, cause-consequence diagrams, diagnostic dictionaries etc.), as opposed to functional models, describe system behavior when faults are present. These models use qualitative representation of faults, discrepancies and their interactions. This is done by discretizing the failure space of the systems in terms of the failure modes of components,

functional discrepancies, alarms etc. Such fault analysis of systems is standard practice in systems engineering (e.g., FMEA, fault trees, etc.) and has been used to diagnose faults. Since our goal is to develop a modeling environment which is based on the concepts and relations used by systems engineers, a fault model representation is better suited for our purpose.

Fault models help in diagnosis by reducing the diagnostic search space. Hypothesis generation is straight-forward – just consider all the failure modes that could have caused the discrepancies. Diagnosing with a single fault assumption is simple. Diagnosing with multiple faults and/or sensor failure assumption can possibly result in a large number of combinations of faults to be examined. In this case, some reasonable heuristics can be used which are derived from the structure of the system.

Fault models using diagnostic dictionaries (the kind used in [7, 8] etc.), provide a simple mapping form faults to effects. The effects of a fault, once all the propagations have taken place and the system has reached a steady state, are listed. Thus, the temporal relationships between faults and the dynamics are lost, making this representation less attractive for FDIR task.

The temporal relationships and the dynamics are captured in the fault models using directed graphs (as in [5, 6]). In the research described in this paper, we use a similar representation. This is done in the following manner (for a more detailed description, see [14, 9]) :

1. Discretize the physical and functional failure space to model only the plausible fault states, called *failure modes* and *discrepancies*, respectively.
2. Discretize the observation space to correspond to the discretized failure space, specifying the discrete *alarms* and *sensor states*. Describe the observation of failures using alarms and sensor states.
3. Specify component and functional boundaries and the input and output failure interfaces.
4. Describe the interactions between failures in terms of *timed failure propagations*, which capture the dynamics of system behavior when it is out of the normal operation range. The uncertainty in dynamics is expressed by using a *propagation interval*. The failure propagations can describe the interactions of failures within a sub-system or between sub-systems.

The above method of modeling faults and their interactions address the challenges of FDIR task outlined earlier. The use of these models for real-time robust diagnostics during system operation is briefly described in the next section.

REAL-TIME ROBUST DIAGNOSTICS: An embedded robust diagnostic system was developed, which is synthesized from the hierarchical fault models. The goal here was to develop diagnostic software which doesn't have a pre-defined structure, but instead, the

structure of the diagnostic system is derived from the structure of the system, as captured in the models. Thus, the overall diagnostic system consists of many monitoring and diagnostic sub-systems, as shown in Figure 1.

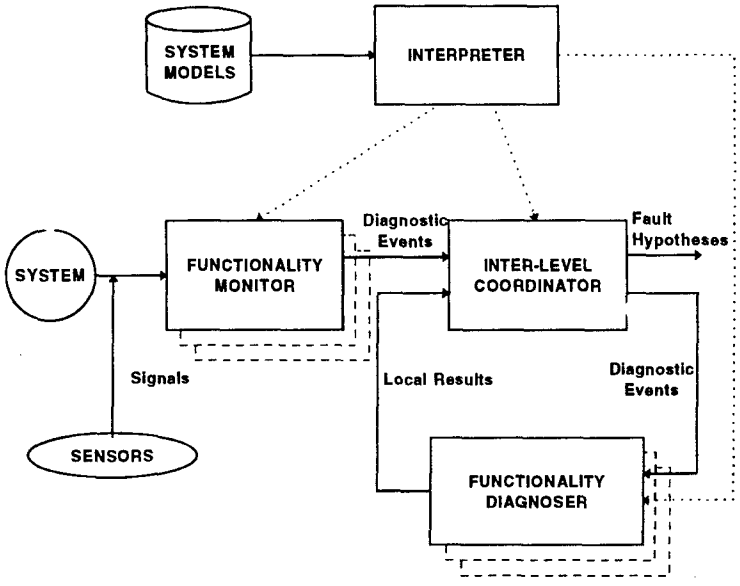

Figure 1: Block Diagram of Robust Diagnostic System

The diagnostic system structure is determined by the functional hiererachy in the models. For each functionality, a monitoring sub-system, the Functionality Monitor (FM), and a diagnostic sub-system, the Functionality Diagnoser (FD), is generated. The interfaces of these sub-systems are determined by the interfaces in the models. An FM receives the sensor signals pertinent to the functionality it represents (as specified in the model of the functionality). If and alarm condition exists, or if the sensor signatures change, the FM generates "diagnostic events" and sends them to the Inter-Level Coordinator (ILC). The FDs are also generated according to the functional breakdown, and there is one FD for each functionality. The interfaces of the FDs (incoming and outgoing failures and diagnostic events) are determined by the respective functionality models.

The ILC (1) receives the diagnostic events from the FMs, (2) routes the events to the proper FDs, (3) controls and guides diagnostic search (4) receives the *local* diagnostic results from FDs (5) combines the local diagnostic results and generates the fault hypotheses.

The prominent features of the diagnostic system are :

- Diagnosis of multiple faults (no assumption of single or multiple points of failures).
- Identification of observation errors.

- Robustness against a large number of sensor failures and graceful degradation as the number of sensor failures increase.
- It is event-driven and uses incremental non-monotonic reasoning.
- It predicts future events and uses the predictor-corrector principle to revise its hypotheses.
- Restricts the diagnostic search to the relevant parts of the functional hierarchy.
- Identifies loss of model validity in case of large faults and restricts its search to those parts of the hierarchy where the model of the system seems to be valid.
- Uses algorithms of polynomial complexity.

For details of the robust diagnostic system and the algorithms used, please see [9, 10].

CONCLUSION: A model-integrated approach to FDIR of complex, large-scale systems was presented. Although the primary motivation for this research came from the FDIR requirements for ISSA, the approach used here could be used for a variety of engineering systems, since it provides a solution approach for FDIR modeling and embedded health management for any complex, large-scale engineering system. The modeling formalisms are derived from standard engineering practices and domain specific concepts and relations, thus making it more accessible to systems engineer. The structural and functional organization of models makes the complexity and the scale of the systems easier to tackle. The feasibility of the model-integrated approach for using design information to formally and automatically derive embedded health management systems is demonstrated by the real-time robust diagnostic system synthesized from the models.

References

[1] E. Scarl *et al.*, "Diagnosis and Sensor Validation through Knowledge of Structure and Function," *IEEE Trans. Syst., Man and Cybernetics*, vol. SMC-17, no. 3, May./June 1987, pp. 360-368.

[2] J. de Kleer and B. C. Williams, "Diagnosing Multiple Failures," *Artificial Intelligence*, vol. 32, 1987.

[3] R. Davis, "Diagnostic Reasoning Based on Structure and Behavior," *Artificial Intelligence*, vol. 24, 1984.

[4] B. Kuipers, "Qualitative Simulation as Causal Explanation," *IEEE Trans. Syst., Man and Cybernetics*, vol. SMC-17, no. 3, May./June 1987, pp. 432-444.

[5] N. H. Narayanan and N. Vishwanadham, "A Methodology for Knowledge Acquisition and Reasoning in Failure Analysis of Systems," *IEEE Trans. Syst., Man and Cybernetics*, vol. SMC-17, no. 2, Mar./Apr. 1987, pp. 274-288.

[6] Padalkar, S., Karsai, G., Biegl, C., Sztipanovits, J., Okuda, K., Miyasaka, N.: "Real-Time Fault Diagnostics," *IEEE Expert,* pp. 75-85, June, 1991.

[7] S. J. Chang, F. DiCesare and G. Goldbogen, *Evaluation of Diagnosability of Failure Knowledge in Manufacturing Systems*, Proceedings, 1990 IEEE International Conference on Robotics and Automation, Vol 1, pp. 696-701.

[8] Pattipati, Krishna R. and Alexandridis, Mark G., "Application of Heuristic Search and Information Theory to Sequential Fault Diagnosis," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 20, no. 4, July/August 1990, pp. 872-887.

[9] Misra, A., "Sensor-Based Diagnosis of Dynamical Systems," Ph.D. Dissertation, Vanderbilt University, May 1994.

[10] Misra, A., Sztipanovits, J., Carnes, R.: "Robust Diagnostic System: Structural Redundancy Approach," in Proc. of the SPIE's International Symposium on Knowledge-Based Artificial Intelligence Systems in Aerospace and Industry, Orlando, FL, April 5-6, 1994.

[11] R. Patton, P. Frank and R. Clark, "Fault Diagnosis in Dynamic Systems: Theory and Application," Prentice Hall International (UK), 1989.

[12] Shogo Tanaka, "Diagnosability of Systems and Optimal Sensor Location," Chapter 5 in the book *Fault Diagnosis in Dynamic Systems: Theory and Application*, Prentice Hall International (UK), 1989, pp. 21-45.

[13] Andow, P. K., and F. P. Lees, "Process Computer Alarm Analysis: Outline of a Method Based on List Processing," *Trans. Inst. Chem. Eng.*, 53, 195 (1975).

[14] Misra A., J. Sztipanovits, Carnes, J. R., "Modeling Paradigm for Failure Detection, Isolation and Recovery," Technical Report #95-001, Measurement and Control Systems Laboratory, Department of Electrical Engineering, Vanderbilt University, Jan. 1995.

[15] Sztipanovits, Janos *et al.*, "MULTIGRAPH: An Architecture for Model-Integrated Computing," submitted to ICECCS 95, Int'l Conf. on Eng. of Complex Systems, Nov. 6-10, 1995.